

Cryptographic Methods of Information Protection

Curs

Tema	Nr. de ore
1. Introduction to Cryptography	2
2. Classical ciphers	2
3. Modern stream ciphers	2
4. Modern block ciphers	4
5. Hash Functions	4
6. Message Authentication Codes	2
7. Basic public key encryption algorithms	4
8. Signature schemes	4
9. Security issues of encryption algorithms	2
10. Steganographic methods in information protection.	2

Laborator

Tematica seminarelor și lucrărilor de laborator (14+16 ore)

Lucrările de laborator vor urmări îndeaproape tematica prezentată la curs, și vor consta în elaborarea aplicațiilor software care implementează algoritmi criptografici propuși de profesor pentru tematica respectivă. Aplicațiile vor fi realizate în mediile studiate de studenții în cursurile anterioare.

Tema	Nr. de ore
1. Classical ciphers	6
2. Modern block ciphers	6
3. Hash Functions and Message Authentication Codes	6
4. Basic public key encryption algorithms	6
5. Signature schemes	6